

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-251375

(43)Date of publication of application : 06.09.2002

(51)Int.Cl.

G06F 15/00

H04L 9/32

(21)Application number : 2001-044841

(71)Applicant : NTT DATA CORP

(22)Date of filing : 21.02.2001

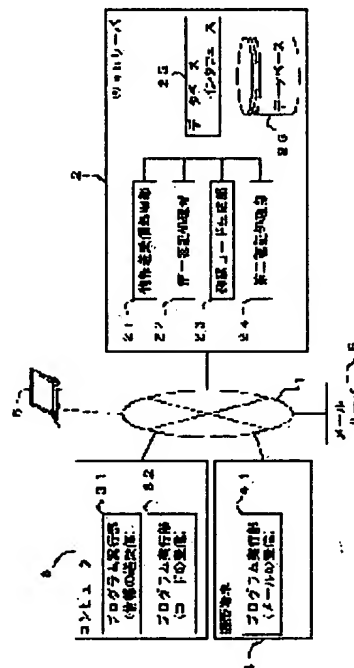
(72)Inventor : GOHIYAKUDEN TAKAYUKI

## (54) USER AUTHENTICATION SERVER IN COMMUNICATION NETWORK, INDIVIDUAL AUTHENTICATION METHOD AND PROGRAM

## (57)Abstract:

PROBLEM TO BE SOLVED: To eliminate illegal 'pretence' and to securely decide a user oneself.

SOLUTION: A Web server 2 receives ID and a password from the computer 3 of the user, collates them with ID and the password, which are stored in a database 26, and performs first authentication. When the first authentication succeeds, the Web server 2 transmits a confirmation code to an electronic mail address which is stored in the database 26 and which the user designates. The destination is a mail server 5. The user receives the confirmation code from the mail server 5 by using a portable terminal 4 and inputs it to a computer 3. The inputted confirmation code is returned to the Web server 2 as a return code. The Web server 2 collates the received confirmation code with the transmitted confirmation code. When they are matched, it is decided that second authentication is succeeded.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

BEST AVAILABLE COPY



## 1

## 【特許請求の範囲】

【請求項1】通信ネットワークに接続され、当該通信ネットワークに接続されたユーザ端末との間で、当該ユーザ端末を使用するユーザの認証を行うためのユーザ認証サーバにおいて、ユーザの認証コードと確認コード送信先とを対応付けて予め記憶する記憶手段と、前記ユーザ端末から送信される認証コードを受信し、受信した認証コードを、前記記憶手段に記憶されている認証コードと照合することにより第1の認証を行う第1の認証手段と、該第1の認証手段による認証が成功したとき、対応する確認コード送信先に、所定の確認コードを通知する確認コード通知手段と、該確認コード通知手段による確認コード通知の応答としての返信コードを受信し、受信した返信コードを、通知した確認コードと照合することにより第2の認証を行う第2の認証手段と、を備えたことを特徴とする通信ネットワークにおけるユーザ認証サーバ。

【請求項2】前記返信コードの送信元は、前記確認コード送信先と異なることを特徴とする請求項1に記載の通信ネットワークにおけるユーザ認証サーバ。

【請求項3】前記第2の認証手段は、受信した返信コードを、前記確認コード通知手段が通知した確認コードと照合した結果、返信コードと確認コードとの間に一定の相関がとれたときに第2の認証を行うものであることを特徴とする請求項1又は2に記載の通信ネットワークにおけるユーザ認証サーバ。

【請求項4】通信ネットワークにおける本人認証方法であって、ユーザの認証データと確認コード送信先とを対応付けてユーザ認証サーバに予め記憶しておくステップと、通信ネットワークを介して受信した認証データを、ユーザ認証サーバに記憶された認証データと照合することにより、認証コードの送り主がユーザ本人であるか否かの認証を行うステップと、認証データの送信主がユーザ本人であるとの認証がなされたとき、通信ネットワークを介して、対応する確認コード送信先に所定の確認コードを通知するステップと、該確認コード通知の応答としての返信コードを受信し、受信した返信コードを、通知した確認コードと照合することにより、前記認証コードの送り主が、前記確認コード送信先に所在するユーザ本人であるかどうかの認証を行うステップと、を備えたことを特徴とする通信ネットワークにおける本人認証方法。

【請求項5】通信ネットワークに接続されたコンピュータに、ユーザの認証コードと確認コード送信先とを対応付けて予め記憶する手順、

## 2

通信ネットワークを介して認証コードを受信して、受信した認証コードを、記憶している認証コードと照合することにより、認証コードの送り主がユーザ本人であるか否かの認証を行う手順、

認証コードの送り主がユーザ本人であるとの認証がなされたとき、対応する確認コード送信先に、所定の確認コードを通知する手順、

確認コード通知の応答としての返信コードを受信して、受信した返信コードを、通知した確認コードと照合することにより、前記認証コードの送り主が、確認コード送信先に所在するユーザ本人であるか否かの認証を行う手順、を実行させるためのプログラム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、通信ネットワークにおけるユーザ認証サーバ、本人認証方法及びプログラム(program)に関し、特に不正ななりすましを防止する通信ネットワークにおけるユーザ認証サーバ、本人認証方法及びプログラムに関する。

## 【0002】

【従来の技術】インターネットは、不特定多数の者が利用することのできる便利な通信ネットワークである。その反面、このインターネットでは、情報伝送路がネットワーク状になっているため、情報は数多くの中継点を經由する。このため、情報が第三者によって不正に盗み取られるという可能性も否定できない。

【0003】このようなインターネットにおいて、不正を防止するためには、まず、通信相手がユーザ本人であるかどうかを確認する必要がある。従来、インターネット上の取引においては、本人認証として、ユーザのIDとパスワードを入力することによりユーザ本人であるかどうかの本人確認を行うのが一般的である。

## 【0004】

【発明が解決しようとする課題】ところで、インターネット上では、ユーザのIDやパスワードを盗み、盗んだIDやパスワードを用いてユーザ本人になりすますような不正行為が見受けられる。このような行為はいわゆる「なりすまし」と呼ばれるものであり、従来の本人認証のやり方では、このような「なりすまし」を防止することは困難である。インターネットでは、この「なりすまし」が大きな脅威であり、このような不正を防止する必要がある。

【0005】本発明は、このような従来の問題に鑑みてなされたもので、不正ななりすましを防止することが可能な通信ネットワークにおけるユーザ認証サーバ、本人認証方法及びセキュリティプログラムを提供することを目的とする。

## 【0006】

【課題を解決するための手段】上記目的を達成するため、本発明の第1の観点に係る通信ネットワークにお

## 3

るユーザ認証サーバは、通信ネットワークに接続され、当該通信ネットワークに接続されたユーザ端末との間で、当該ユーザ端末を使用するユーザの認証を行うためのユーザ認証サーバにおいて、ユーザの認証コードと確認コード送信先とを対応付けて予め記憶する記憶手段と、前記ユーザ端末から送信される認証コードを受信し、受信した認証コードを、前記記憶手段に記憶されている認証コードと照合することにより第1の認証を行う第1の認証手段と、該第1の認証手段による認証が成功したとき、対応する確認コード送信先に、所定の確認コードを通知する確認コード通知手段と、該確認コード通知手段による確認コード通知の応答としての返信コードを受信し、受信した返信コードを、通知した確認コードと照合することにより第2の認証を行う第2の認証手段と、を備えたものである。

【0007】このような構成によれば、第1の認証手段による第1の認証が成功したときは、確認コードが送信される。確認コードは、対応するユーザの認証コードに対応した確認コード送信先に送信されるので、第三者がユーザの認証コードを盗んでユーザになりすますことにより、第1の認証がうまく成功したとしても、この第三者には、確認コードは届かない。確認コードが届かなければ、第三者は返信コードを送信することもできず、返信コードが受信されなければ、確認コードと返信コードとの照合を行うことはできず、第2の認証手段による第2の認証を行うことはできない。これにより、なりすましは排除され、不正が防止される。

【0008】前記返信コードの送信元は、前記確認コード送信先と異なるようにしてもよい。また、前記第2の認証手段は、受信した返信コードを、前記確認コード通知手段が通知した確認コードと照合した結果、返信コードと確認コードとの間に一定の相関がとれたときに第2の認証を行うものであってもよい。

【0009】本発明の第2の観点に係る通信ネットワークにおける本人認証方法は、ユーザの認証データと確認コード送信先とを対応付けてユーザ認証サーバに予め記憶しておくステップと、通信ネットワークを介して受信した認証データを、ユーザ認証サーバに記憶された認証データと照合することにより、認証コードの送り主がユーザ本人であるか否かの認証を行うステップと、認証データの送信主がユーザ本人であるとの認証がなされたとき、通信ネットワークを介して、対応する確認コード送信先に所定の確認コードを通知するステップと、該確認コード通知の応答としての返信コードを受信し、受信した返信コードを、通知した確認コードと照合することにより、前記認証コードの送り主が、前記確認コード送信先に所在するユーザ本人であるかどうかの認証を行うステップと、を備えたものである。

【0010】本発明の第3の観点に係るプログラムは、通信ネットワークに接続されたコンピュータに、ユーザ

## 4

の認証コードと確認コード送信先とを対応付けて予め記憶する手順、通信ネットワークを介して認証コードを受信して、受信した認証コードを、記憶している認証コードと照合することにより、認証コードの送り主がユーザ本人であるか否かの認証を行う手順、認証コードの送り主がユーザ本人であるとの認証がなされたとき、対応する確認コード送信先に、所定の確認コードを通知する手順、確認コード通知の応答としての返信コードを受信して、受信した返信コードを、通知した確認コードと照合することにより、前記認証コードの送り主が、確認コード送信先に所在するユーザ本人であるか否かの認証を行う手順、を実行させるためのものである。

【0011】

【発明の実施の形態】以下、本発明の実施の形態に係る通信ネットワークにおけるセキュリティシステムを図面を参照して説明する。図1は、本実施の形態に係るセキュリティシステムの構成を示すブロック図である。この実施の形態に係るセキュリティシステムは、インターネット1と、Webサーバ2と、コンピュータ3と、携帯端末4と、メールサーバ5と、を備えている。尚、コンピュータ6は、ユーザ本人になりすまして不正に情報を送受信しようとする第三者のコンピュータである。

【0012】インターネット1は、情報を送受信するためのネットワークである。Webサーバ2は、インターネット1に接続されて、ユーザのID及びパスワード等の情報をHTTP (HyperText Transfer Protocol) プロトコルに従って送受信するためのコンピュータである。

【0013】Webサーバ2は、情報送受信処理部21と、第一認証処理部22と、確認コード生成部23と、第二認証処理部24と、データベースインタフェース25と、データベース26と、を備えて構成されている。

【0014】情報送受信処理部21は、ユーザのコンピュータ3との間で情報の送受信を行うものである。第一認証処理部22は、ユーザから送信されたID、パスワードを、データベース26に記憶されているユーザのID、パスワードと照合し、照合結果に基づいて第一認証を行うものである。

【0015】確認コード生成部23は、第一認証処理部22によって第一認証が行われた後に、確認コードを自動的に生成するものであり、生成した確認コードをデータベースインタフェース25を介してデータベース26に記録する。確認コードは、後述するように、送り先のユーザと対応する記憶場所に記憶される。第二認証処理部24は、ユーザに送信した確認コード及びユーザから返送された返信コードを照合し、照合結果に基づいて第二認証を行う処理部である。データベースインタフェース25は、ユーザのID、パスワード、送信した確認コード等をデータベース26に記録し、データベース26から読み出すものである。

## 5

【0016】データベース26は、ユーザのID、パスワード、ユーザが指定した電子メールアドレス等のユーザ情報をユーザごとに対応付けて記憶しておくためのものである。図2は、データベース26に記憶されたユーザ情報の一例を示す説明図である。図2に示すように、データベース26には、ユーザ毎にユーザエリアが設けられ、各ユーザエリアには、ユーザ名、ユーザのID、パスワード、電子メールアドレス等が記憶される。前述の確認コード等もこのユーザエリアに記憶される。

【0017】電子メールアドレスは、認証成功のメッセージ、確認コード等、ユーザに送るメールの送り先を指定するためのものであり、ユーザ自身によって指定される。この電子メールアドレスによってメールサーバ5が指定される。

【0018】コンピュータ3は、ユーザが使用するコンピュータであり、インターネット1に接続されている。コンピュータ3は、プログラム実行部31及びプログラム実行部32を有している。プログラム実行部31は、情報の送受信処理プログラムを実行する実行部である。この送受信処理プログラムは、Webサーバ2との間で送受信を行えるようにブラウザ機能を有している。また、プログラム実行部32は、メールサーバ5に届けられたメールを受信するための受信処理プログラムを実行する実行部である。

【0019】図3は、コンピュータ3のハードウェア構成を示すブロック図である。コンピュータ3は、CPU (Central Processing Unit) 33と、ROM (Read Only Memory) 34と、RAM (Random Access Memory) 35と、ディスプレイ36と、キーボード37と、マウス38と、HDD (Hard Disk Drive) 39と、を備えている。

【0020】CPU33は、プログラム実行部31及びプログラム実行部32を実行するためのものである。ROM34は、プログラム実行部31及びプログラム実行部32によって実行されるプログラムを格納しておくためのメモリである。RAM35は、プログラム実行部31及びプログラム実行部32の実行に必要なデータを一時格納しておくためのメモリである。

【0021】ディスプレイ36は、Webサーバ2から送信された情報を表示し、データ入力の案内を表示するためのものである。キーボード37は、ID、パスワードを入力するためのものである。マウス38は、ディスプレイ36に表示された各ボタンをクリックするためのものである。HDD39は、Webサーバ2との間で送受信した情報を格納しておく記憶装置である。

【0022】携帯端末4は、携帯可能な端末であり、しかも通信機能を備えたものである。携帯端末4には、例えば、携帯電話、PHS (Personal Handyphone System)、PDA (Personal Digital Assistance)、モバイル (Mobile) コンピュータが含まれる。この携帯端末4

## 6

は、プログラム実行部41を有している。プログラム実行部41は、メールサーバ5に届けられたメールを受信するための受信処理プログラムを実行する実行部である。

【0023】携帯端末4には、液晶ディスプレイと、ダイヤルキーと、スピーカと、マイクと、アンテナと、が備えられている。液晶ディスプレイは、送受信情報、操作情報等を表示するためのものである。ダイヤルキーは、発呼手続等を行うためのものである。スピーカは、受信した音声を出力するためのものである。マイクは、ユーザの声を入力するためのものである。アンテナは、通話信号を送受信するためのものである。メールサーバ5は、Webサーバ2から送信されたメール、確認コードを記憶しておくものである。

【0024】次に、本実施の形態に係るなりすましを排除するための本人認証方法について説明する。図4は、本実施の形態に係るWebサーバ2、コンピュータ3及び携帯端末4の動作を示すフローチャートである。

【0025】まず、コンピュータ3では、プログラム実行部31が、Webサーバ2にログインの要求をする (ステップS11)。Webサーバ2では、情報送受信処理部21が、コンピュータ3から送信されたログイン要求を取得し (ステップS12)、ログイン要求ページをコンピュータ3に送信する (ステップS13)。

【0026】コンピュータ3では、プログラム実行部31が、Webサーバ2から送信されたログイン要求ページを受信し、受信したログイン要求ページをコンピュータ3のディスプレイ36に表示する (ステップS14)。

【0027】図5は、コンピュータ3のディスプレイ36に表示されたログイン要求ページの表示例を示す説明図である。ディスプレイ36には、図5(a)に示すように、「お客様のIDとパスワードを入力して下さい。」とのメッセージとともに、ID、パスワードの入力枠、「OK」ボタン、「再入力」ボタンが表示される。

【0028】ユーザは、この表示に従ってキーボード37を操作し、ID、パスワードの入力枠に、それぞれID、パスワードを入力する。ID又はパスワードを間違えたとき、ユーザは、「再入力」ボタンをクリックし、ID又はパスワードを入力し直す。正しければ、「OK」ボタンをクリックする。

【0029】「OK」ボタンがクリックされたとき、プログラム実行部31は、ID及びパスワードをWebサーバ2に送信する (ステップS15)。Webサーバ2では、情報送受信処理部21が、コンピュータ3からユーザのID及びパスワードを受け取る (ステップS16)。

【0030】第一認証処理部22は、予め記憶されているユーザID及びパスワードを、データベースインタフ

ューズ 25 を介してデータベース 26 から取り出し、受け取ったユーザ ID 及びパスワードを、予め記憶されているユーザ ID 及びパスワードと照合する（ステップ S 17）。

【0031】図 2 に示すように、データベース 26 には、ユーザ A の ID、パスワードとして、それぞれ「a b c 1 2 3」、「RESUONOTNOH」が記憶されている。受け取った ID が「a b c 1 2 3」であり、パスワードが「RESUONOTNOH」であるときは、照合した結果、受け取った ID 及びパスワードは、データベース 26 に記憶された ID 及びパスワードと一致する。一致したとき、第一認証処理部 22 は、第一認証が成功したと判定する（ステップ S 18）。

【0032】一方、受け取った ID が「a b c 1 2 3」であり、パスワードが「RESUONESIN」であるときは、照合した結果、受け取った ID 及びパスワードは、データベース 26 に記憶された ID 及びパスワードと一致しない。一致しなかったとき、第一認証処理部 22 は、第一認証不成功と判定する。

【0033】第一認証が不成功と判定されたとき、情報送受信処理部 21 は、再度、確認のため、ログイン要求ページをコンピュータ 3 に送信し（ステップ S 13）、送信されたユーザ ID 及びパスワードを受け取って（ステップ S 16）、照合を行い（ステップ S 17）、第一認証成功可否かの判定を行う（ステップ S 18）。

【0034】所定回数、第一認証が不成功に終わったとき、ログインを要求した者は、不正にアクセスした者とみなしてこの処理を終了させる。このようにして、不正なアクセスが防止される。

【0035】第一認証が成功したとき、確認コード生成部 23 が、確認コードを自動生成する（ステップ S 19）。確認コードは、数値、文字、記号のいずれか、あるいはこれらの組み合わせによってランダムに生成される。情報送受信処理部 21 は、確認コード生成部 23 によって生成された確認コードを、データベース 26 に記憶されている電子メールアドレスの宛先へ送信する（ステップ S 20）。

【0036】例えば、ユーザ A の場合、前述のように電子メールアドレスは、「user\_a@ichinonet.ne.jp」になっているので、確認コードは、ユーザ A によって指定されたメールサーバ 5 に送信される。尚、送信した確認コードは、データベースインタフェース 25 によって、データベース 26 の確認コード記憶エリアに記憶される。

【0037】ユーザは、メールを受信するため、携帯端末 4 を操作し、携帯端末 4 は、メールサーバ 5 にアクセスして、確認コードが記録されたメールを受信する（ステップ S 21）。Web サーバ 2 では、情報送受信処理部 21 が、取引案内ページをコンピュータ 3 に送信する（ステップ S 22）。

【0038】コンピュータ 3 では、プログラム実行部 3

1 が、取引案内ページを受信し（ステップ S 23）、この取引案内ページをディスプレイ 36 に表示する。ディスプレイ 36 には、図 5（b）に示すように、案内メッセージ「お取引の種別を入力して下さい。」が表示され、取引内容として、種別 1～3 が表示される。例えば、取引が金融機関における取引の場合、種別 1～2 は、残高照会、振り替え等となる。

【0039】ユーザは、この表示に従ってキーボード 37 を操作し、取引の種別を入力する。種別を間違えたとき、ユーザは、「再入力」ボタンをクリックし、正しければ、「OK」ボタンをクリックする。

【0040】「OK」ボタンがクリックされたとき、プログラム実行部 31 は、入力された取引の種別を Web サーバ 2 に送信し、取引依頼の要求をする（ステップ S 24）。Web サーバ 2 では、情報送受信処理部 21 が、コンピュータ 3 から送信された取引依頼の要求を受信する（ステップ S 25）。

【0041】第二認証処理部 24 は、取引内容が第二認証を要するものかどうかを判定する（ステップ S 26）。例えば、取引が金融機関における取引であって、取引内容が残高照会等の場合のように、セキュリティを強化すべきではないときは、第二認証を行う必要はないと判定し、第二認証を実行せずに、取引ページをコンピュータ 3 に送信する（ステップ S 35）。

【0042】一方、取引内容が自分の口座から他人の口座への振り替えの場合のように、セキュリティを強化すべき場合、第二認証処理部 24 は、第二認証を行う必要があると判定する。第二認証処理部 24 が第二認証を要すると判定したとき、情報送受信処理部 21 に確認コード要求ページを送信する（ステップ S 27）。

【0043】コンピュータ 3 では、プログラム実行部 31 が確認コード要求ページを受信する（ステップ S 28）。図 5（c）に示すように、コンピュータ 3 のディスプレイ 36 には、「確認コードを入力して下さい。」とのメッセージとともに、確認コードを入力する入力枠が表示される。

【0044】携帯端末 4 では、確認コードがユーザによって取得され（ステップ S 29）、コンピュータ 3 では、ユーザによって確認コードが入力され（ステップ S 30）、入力された確認コードは入力枠に表示される。この確認コードを入れ間違えたとき、ユーザは、「再入力」ボタンをクリックし、正しければ、「OK」ボタンをクリックする。

【0045】「OK」ボタンがクリックされたとき、コンピュータ 3 のプログラム実行部 31 は、入力された確認コードを返信コードとして Web サーバ 2 に送信する（ステップ S 31）。

【0046】Web サーバ 2 では、コンピュータ 3 から送信された確認コードを受信する（ステップ S 32）。ここで、ユーザになりすまして、ID 及びパスワードを

Webサーバ2に送信したとしても、この者は、データベース26に記憶されている電子メールアドレスを知ることにはできない。従って、ユーザになりすました者は、確認コードを返信することはできず、確認コードが返信されなかったとき、第二認証処理部24は、処理を終了させる。確認コードを受信したとき、第二認証処理部24は、送信した確認コードをデータベース26の確認コード記憶エリアから取り出す。そして、第二認証処理部24は、受信した確認コードを、送信した確認コードと照合する(ステップS33)。

【0047】ID及びパスワードの送り主がユーザ本人であれば、Webサーバ2から送信された確認コードと同じ確認コードが返信されるので、送信した確認コードと受信した確認コードとが一致することになる。確認コードが一致したとき、第二認証処理部24は、第二認証が成功したと判定する(ステップS34)。

【0048】一方、確認コードが一致しなかったときは、入力ミスも考えられるため、再度、確認コード表示ページを送信し(ステップS27)、確認コードを受信して(ステップS32)、再度、照合を行う(ステップS33)。そして、照合の結果、所定回数、不一致が続いたときは、ユーザ本人になりすました者が適当に確認コードをWebサーバ2に送信していることも想定されるため、第二認証は、最終的に不成功と判定し、この処理を終了させる。このようにして、なりすましが排除される。第二認証が成功したと判定されたとき(ステップS34)、情報送受信処理部21は、取引ページを送信する(ステップS35)。

【0049】コンピュータ3では、プログラム実行部31が、取引ページを受信し、この取引ページをコンピュータ3のディスプレイ36に表示する(ステップS36)。コンピュータ3のディスプレイ36には、図5(d)に示すように、第二認証の成功メッセージとして「お客様であることを確認できました。」が表示され、ユーザとの間で取引等が開始される。

【0050】以上説明したように、本実施の形態によれば、ID及びパスワードを受け取って第一認証が成功したときは、確認コードを自動生成して、ユーザが指定した電子メールアドレス宛て(メールサーバ5)に送信し、その応答として受信した確認コードを、送信した確認コードと照合することにより、第二認証を行うようにしたので、不正な「なりすまし」を排除してユーザ本人の確定を確実に行うことができる。これにより、インターネット上でのセキュリティを強化することができる。

【0051】尚、本発明を実施するにあたっては、種々の形態が考えられ、上記実施の形態に限られるものではない。例えば、上記実施の形態のように、通信ネットワークは、インターネット1ではなく、イントラネット(intranet:企業内ネットワーク)であってもよい。通信ネットワークがインターネット1である場合は、HT

TPプロトコルに従ってデータを送受信できるように、Webサーバ2を用いたのに対し、イントラネットでは、サーバに、データを所有しているデータベースサーバ、あるいは受信した情報とデータベースとを関連づけて処理をするようなアプリケーションサーバ等を用いることもできる。これらのサーバを用いた場合には、これらのサーバが、ユーザからのアクセスに対して直接、第一認証、第二認証を行うことになる。

【0052】コンピュータ3と携帯端末4との機能については、携帯端末4にブラウザ機能を備え、メールサーバ5に届けられたメールをコンピュータ3で受信し、各ページの受信、ID、パスワード及び確認コードの送信を携帯端末4で行えるようにすることもできる。

【0053】確認コード生成部23は、確認コードを必ずしもランダムに生成するように構成されたものでなくともよく、例えば、数字、記号等を連番にして確認コードを生成するものであってもよい。

【0054】コンピュータ3から返信する確認コードは、必ずしもWebサーバ2から送信された確認コードと同じである必要はなく、Webサーバ2が送信した確認コードとコンピュータ3から返信された確認コードとの間に相関がとれるようにしてあれば良い。例えば、コンピュータ3のプログラム実行部31が確認コードの文字列を逆にして返信することもできるし、プログラム実行部31が、所定の規則に従って(例えば、連番で)コードを作成して返信することもできる。また、Webサーバ2が確認コードを暗号化して送信し、受信した確認コードを復号化するようにしてもよい。

【0055】確認コードを送るタイミングについては、上記実施の形態では、第一認証が成功したとき、すぐに送るようにしたが、第二認証が必要かどうかを判断してから送るようにしてもよい。上記実施の形態の適用対象としては、必ずしも金融機関に限られるものではなく、個人的な情報交換等も含め、様々なものに適用することができる。

【0056】さらに、上記実施の形態では、プログラムが、それぞれメモリに予め記憶されているものとして説明した。しかしながら、これらのプログラムは、FD(Floppy Disk)、CD-ROM(Compact Disc Read-Only Memory)、DVD(Digital Video Disc)などのコンピュータ読み取り可能な記録媒体に格納して配布するものとしてもよい。そして、インターネット上のサーバ装置が有するディスク装置等にプログラムを格納しておき、例えば、搬送波に重畳させて、コンピュータにダウンロード等するものとしてもよい。

【0057】

【発明の効果】以上説明したように、本発明によれば、不正を防止することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係るセキュリティシステ

ムの構成を示すブロック図である。

【図2】図1のデータベースに記憶されたユーザ認証情報の一例を示す説明図である。

【図3】図1のコンピュータのハードウェア構成を示すブロック図である。

【図4】本発明の実施の形態に係るWebサーバ、コンピュータ及び携帯端末の動作を示すフローチャートである。

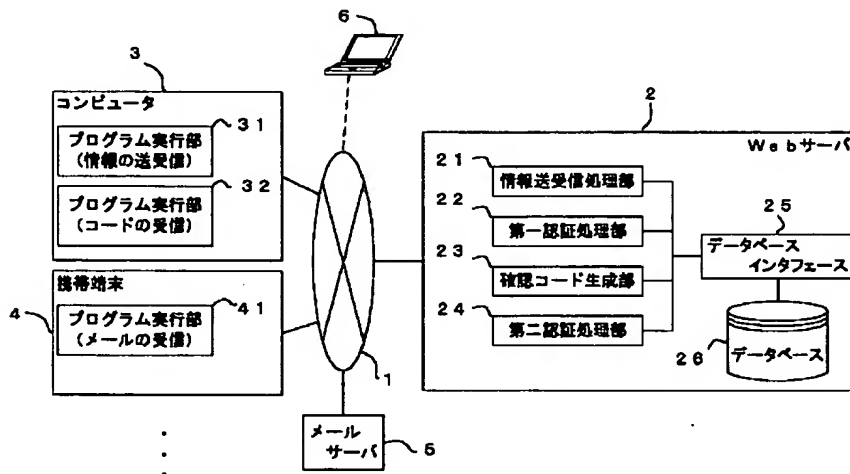
【図5】図1のコンピュータのディスプレイに表示された表示例を示す説明図である。

# 【符号の説明】

- 1 インターネット
- 2 Webサーバ
- 3 コンピュータ
- 4 携帯端末
- 5 メールサーバ
- 22 第一認証処理部
- 24 第二認証処理部
- 31, 32, 41 プログラム実行部

10

【図1】

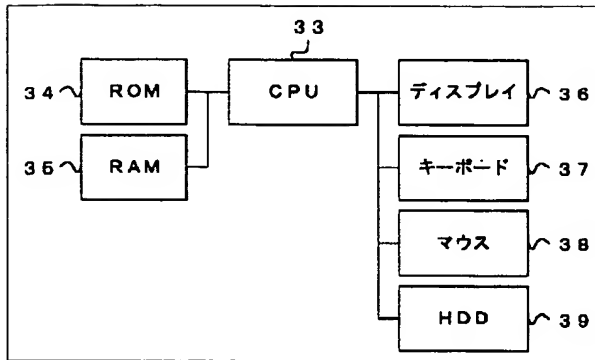


【図2】

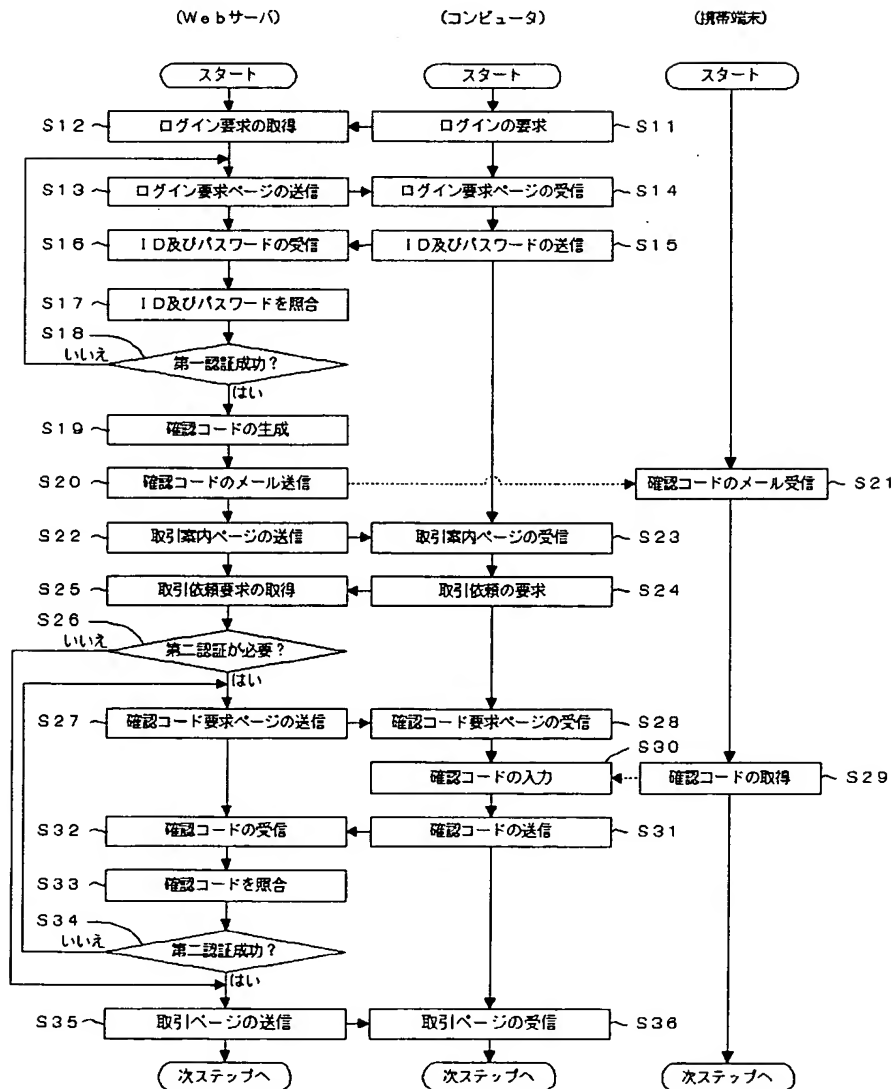
ユーザ	ID	パスワード	電子メールアドレス	(確認コード記憶エリア)	...
A	abc123	***** (RESUONOTNOH)	user_a@ichinonet.ne.jp		...
B	cfig456	*****	user_b@nino_net.ne.jp		...
C	hij789	*****	user_c@sannonet.ne.jp		...
					...



【図3】



【図4】



【図 5】

(a)

お客様のIDとパスワードを  
入力して下さい。

ID

パスワード

(b)

お取引引きの種別を入力して下さい。

(c)

確認コードを入力して下さい。

(d)

お客様であることを確認できました。